White Paper

Overview

Virtual Private Network (VPN)

What is a VPN?

A Virtual Private Network (VPN) utilizes a public network, such as the Internet, to transmit private data.

The cost advantages of a virtual private network:

- Decreases costs associated with traditional remote access solutions
- Reduces infrastructure cost and complexity by leveraging a company's existing investment in the Internet
- Eliminates access costs such as 800 numbers and long-distance charges

Virtual Private Networks reduce costs by using a public channel for private communications.

When the key to success in a rapidly changing world is often the "bottom line," new technologies offering significant cost savings are quick to be singled out for closer scrutiny. Such is the case with Virtual Private Network (VPN) technology.

VPN technology enables a corporation to use a public network, such as the Internet, for communicating private data.

For companies with multiple locations, telecommuters, mobile workers or the need to exchange information with trading partners, the VPN offers a viable alternative to such traditional remote access solutions as X.25, leased lines, Frame Relay, 800 numbers and long distance modem dial-in.

According to Forrester Research, Inc., as reported in the February 1997 issue of Portable Design, more than half of the Fortune 1000 companies surveyed are planning or committed to opening up their intranets to remote and mobile users via the Internet. Further, the same study reports that having remote users access the corporate Local Area Network (LAN) via the Internet rather than by traditional means will cut remote access costs by as much as two-thirds.

Companies that implement a PC-to-LAN VPN solution not only save on traditional remote access costs, they also save by leveraging their existing investment in the Internet. By consolidating remote access lines into Internet channels, companies can reduce infrastructure complexity and save on administrative and managements costs.

Forging industry standards, the first step toward wide-scale adoption.

The first step in the wide-scale adoption of any new technology involves the creation of industry standards.

Today, a number of operating protocols are vying for acceptance as the de facto standard for VPN technology. Among the leaders are Point-to-Point Tunneling Protocol (PPTP) developed for client-to-LAN access, and Layer Two Forwarding Protocol (L2F), developed for LAN-to-LAN access. A third option, Layer Two Tunneling Protocol (L2TP), combines elements of PPTP and L2F. It's scheduled for release sometime in 1998.

The Internet Engineering Task Force (IETF), the standards body assigned to the role of establishing industry-wide guidelines for the Internet, has introduced its own protocol, IPSec. Although supported by some vendors, IPSec has its limitations; most significant is the fact that it supports IP packets only.

For the foreseeable future, PPTP stands the greatest chance of gaining wide-scale industry acceptance. It provides a non-proprietary solution for remote clients and supports multi-protocol tunneling. In addition, it offers vendors and users the greatest level of flexibility and operating independence.

Extended Systems®

VPNs promise cost savings a

Virtual Private Network

Options for deployment of VPNs:

VPN technology can be implemented in a variety of ways.

Routers and Firewalls with encryption capability.

Pros:
- Encryption upgrades, if available, can be cost effective

Cons:
- Mixing vendor solutions can create compatibility issues that inhibit VPN capability
- May not be able to provide PC-to-LAN capability without additional software support
- Could require commitment to vendor's proprietary technology
- May not provide multi-protocol support
- Installation and configuration can add to network complexity
- Encryption processing overhead may reduce performance

Traditional Remote Access Server (RAS) with VPN add-on.

Pros:
- May allow IT to take advantage of an existing hardware investment

Cons:
- Traditional Remote Access Servers are not optimized for VPN
- VPN add-ons may only be available for some high-end RAS solutions
- May be ISP dependent, requiring the company to adopt the same RAS VPN vendor as the ISP
- May not provide multi-protocol support
- May require vendor proprietary software

NOS /Server-Based VPN

Pros:
- More robust solution for PC-to-LAN access than that provided by firewalls or routers

Cons:
- Difficult to set up and manage VPN functionality
- Adding VPN services to a network server can impact performance while decreasing fault tolerance
- Dedicating a network server to remote access can be prohibitively expensive

VPN Services

Pros:
- Security and performance can be guaranteed for a price
- Requires limited corporate support

Cons:
- IT gives up control to the service provider
- May not provide multi-protocol support
- May not provide PC-to-LAN access
- VPN services may be cost prohibitive

Dedicated VPN Software

Pros:
- Optimized to create LAN-to-LAN-connections via VPN
- Dedicated VPN solution creates fault tolerance
- Standalone VPN-solutions can offer greater performance
- Dedicated VPN-solutions are generally easier to use and support than solutions originally designed for non-VPN functions such as firewalls, routers, network servers and traditional remote access servers
- Eliminates the need for costly frame relay circuits, leased lines, etc.

Cons:
- Vendor proprietary software is needed for each server hosting VPN and each remote client accessing the LAN via VPN
- Must invest in a dedicated server for maximum performance
- Adding VPN software on an existing, in-use network server decreases fault tolerance and performance
- Many solutions support IP-only VPNs and cannot transport packets from multiple protocols

Dedicated VPN Hardware

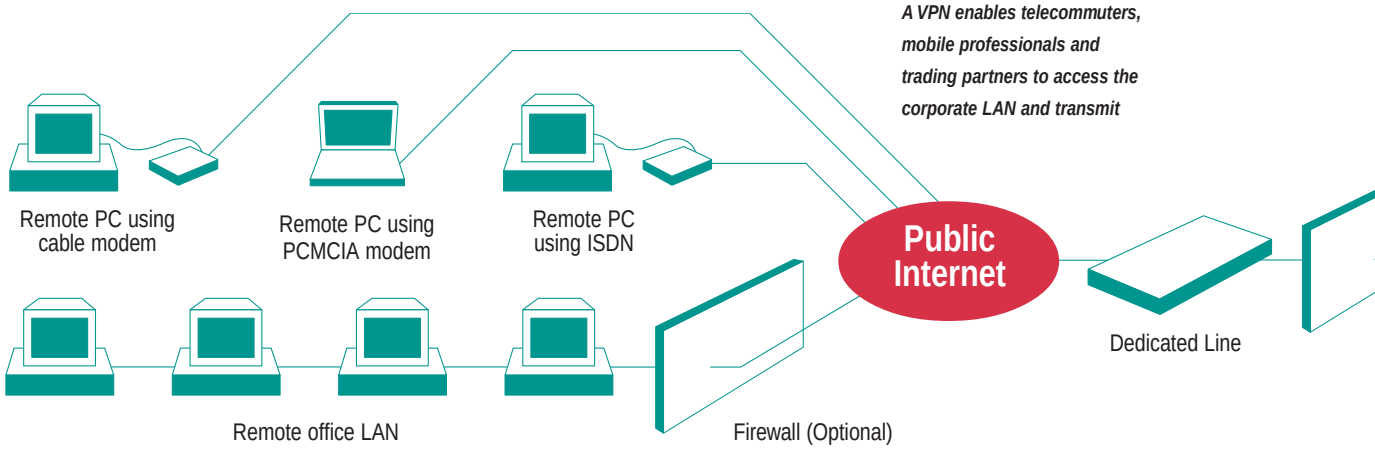
Pros:
- Easy to install, configure and manage
- Saves money by reducing equipment needs at corporate site
- Stand-alone solution offers greater performance and fault tolerance because it is optimized for VPN functionality
- Reduces costs of upgrading hardware as remote access technology changes
- Reduces costs of upgrading system as the number of users increases

Cons:
- Some solutions do not support multiple protocols
- Some LAN-to-LAN VPN solutions require costly software add-ons to support remote client PCs
- Some solutions require that proprietary software be loaded on the remote client's PC

Scalability

Scalability should be of great concern to corporations considering VPN. VPN needs will most certainly change as demand for access to the corporate LAN increases. Therefore it is important to adopt a VPN solution that is flexible in terms of implementation and number of users it supports.

A VPN enables telecommuters, mobile professionals and trading partners to access the corporate LAN and transmit



and more.

Security

One of the most important issues regarding VPN technology is how to assure the security of private data passing through a public channel. Most VPN solutions on the market today offer security for corporate communication needs. VPN security falls into three categories: encryption, authentication and integrity.

Encryption is the function of scrambling data so that only the intended receiver can read it.

Authentication is the process of verifying the sender to the receiver.

Integrity ensures that the data has not been tampered with during transmission.

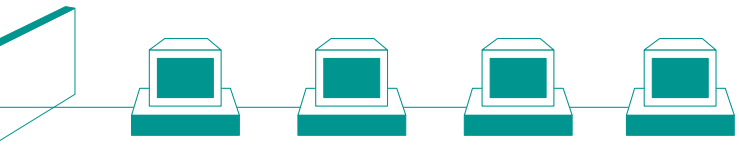
VPN, It's Simply a Matter of Choosing The Right Solution.

Generally speaking, most VPN solutions will reduce infrastructure complexity and contribute to lower operation and maintance costs. However, there are some VPN options that are superior solutions for specific remote access needs, such as PC-to-LAN access. When selecting a VPN solution, regardless of your remote access needs, you should consider the following:

- It should offer multi-protocol support for LAN access
- It should be optimized for VPN-functionality
- It should be easy to set up, configure and manage
- It should offer SNMP-compliant management capability
- It should be easy to upgrade
- It should offer a secure and reliable link to corporate headquarters
- It should be backed by a comprehensive support program

IT managers need to review their network and user needs carefully before selecting a VPN solution. To be successful, companies must choose a migration path that is best suited to their current and future remote access needs.

VPN solutions implement security mechanisms throughout the data flow to ensure that information cannot be accessed, changed or



Firewall (Optional) Corporate LAN

VPN and your Bottom Line

Burgeoning use of the World Wide Web, increased Internet connectivity and the growth of Intranets within companies of all sizes have driven the search for less expensive and cumbersome ways to do business electronically.

Combined with an ever-increasing need for information access due to shifts toward mobile computing and telecommuting, companies have been quick to discover alternatives that would offer the requisite network expansion.

Virtual Private Network technology offers great promise as an exciting and practical new application for the Internet, with easily justifiable and measurable cost savings, particularly as compared to implementing large, private hardware- and management-intensive

VPN, Ready or Not?

Here are a few simple questions that can help you decide whether or not your company is ready for the move to a VPN.

1. *Is your organization fully networked (IP or IPX; Ethernet)*
2. *Does your organization have a dedicated Internet connection?*
3. *Does your company have Windows 95 or Windows NT 4.0 workstation remote clients?*
4. *Does your organization need PC-to-LAN remote access to support mobile professionals and/or telecommuters?*
5. *Are you spending a significant amount of money on dial-in access charges, 800-lines, modem pools and other remote access options?*
6. *Do you want to maintain control of remote access internally?*

If you answered "Yes" *to any of these questions you may be ready to consider a Virtual Private Network solution from Extended Systems.*

For updates and more information on the VPN marketplace and technology developments, please visit the Extended Systems web site at: ***www.extendedsystems.com***

Glossary of terms

Virtual Private Network

Encryption Encryption disguises/scrambles the contents of a message as it travels over a network, making it unintelligible to hackers who may monitor or copy it. Encryption uses a mathematical algorithm and a digital key (series of bits) based on the algorithm to code a message at one end of a transmission and then decode it at the other end.

Firewall Firewalls are barricades at the edge of your company's network to keep intruders from entering. Firewalls can be stand-alone devices or fully integrated firewalls built into routers or remote access servers. They can also be implemented at the application level using proxy gateways and servers.

IETF Internet Engineering Task Force, the official standards body working toward adoption of a finalized set of industry standards by Fall of 1997.

Tunneling A VPN can be created by using "tunneling." Tunneling is a technology that lets a network transport protocol carry information for other protocols within its own packets. For example, IPX data packets can be encapsulated in IP packets for transport across the Internet, which isn't normally possible. The packets may be secured using data encryption, authentication or integrity functions. The packets are delivered unmodified to a remote device that has been set up to handle them.

IPSec IPSec was used initially by Firewall and other security venders. This tunneling protocol supports IP packets only. IPSec takes private IP packets, performs data security functions such as encryption, authentication and integrity, then wraps these secured packets in other IP packets for transport over the Internet.

L2F L2F is a tunneling protocol which was created by Cisco and is incorporated in Cisco's IOS (Internet Operating System). It can support tunneling of IP, IPX or NetBEUI protocols inside IP packets

PPTP PPTP was developed by Microsoft and several remote access vendors. It can support tunneling of IP, IPX or NetBEUI protocols inside IP packets. PPTP was designed for PC-to-LAN remote access.

L2TP L2TP is a tunneling protocol currently under development which will combine Cisco's L2F with Microsoft's PPTP. L2TP makes it possible to have multiple simultaneous tunnels opened between end points. This can ensure a certain degree of quality of service by allowing administrators to dedicate tasks to certain channels. The plan is to have L2TP enabled products shipping by the end of 1998.

ISP Internet Service Provider. Companies that provide access to the Internet.

For additional product information please visit our award-winning Web Site at:

www.extendedsystems.com

E-mail: info@extendsys.com
800-235-7576

Extended Systems®

Extended Systems
5777 N. Meeker Ave.

Extended Systems has been designing and manufacturing highly reliable products backed by exceptional customer service since 1984. Products include Network Print Servers, Printer Sharing, Virtual Private Network Solutions, Infrared Connectivity Solutions, Port Replicators and Client/Server Database Solutions.

9710-0322-9708